CONNECTING TO THE VPN – A TROUBLESHOOTING GUIDE

The VPN Service may be used to connect to NASA internet resources that otherwise may only be accessible from within the IV&V network. In addition, the VPN may be used to establish a secure connection so that a Remote Desktop Connection can be utilized for customers who have a workstation onsite, for customers who are accessing the Terminal Server, or for Virtual Desktop (VDI) customers.

While other agency VPNs make use of Cisco appliances, IV&V uses a Pulse secure VPN for VPN connectivity. If you have not already done so or need to download to reinstall the Pulse Secure VPN software, visit https://www.nasa.gov/centers/ivv/foremployees/employees_ra_requirements.html Guides are available for installing and configuring the Pulse Secure application.

If you are having problems connecting to the VPN, the best way to troubleshoot the problem is to understand at which point your connection is failing and how to properly interpret the system messages you are receiving.

Step 1: Authentication

Use RSA Token or PIV Smartcard.

The VPN uses the Agency Launchpad service to authenticate and you can choose to utilize RSA Token (AUID/password = 8-character PIN (exactly 8 characters) that you have set, followed by the numbers generated from your NASA-issued RSA token) **or** your PIV Smartcard + PIV PIN.

Repeated failure to authenticate may result in a locked account, in which case you will need to contact the IT Help Desk (ivv-dl-help@mail.nasa.gov) for assistance. For after-hours support, you can contact the ESD (https://esd.nasa.gov) for token-related issues, including locked token, PIN resets, and PIN changes.

Error Message: A failure to authenticate will always return an "***Credentials were invalid. Please try again***." message. Any other error is not a result of incorrectly typing your username and password.

Step 2: Securing connection

The second step in successfully connecting to the VPN involves loading the necessary software to complete the connection.

Pulse Secure software is comprised of 3 component applications that are installed on the client computer. The following three (3) components may need to be uninstalled and reinstalled to resolve software issues.

- Pulse Secure 9.1
- Pulse Secure Setup Client (see important note below)
- Pulse Secure Host Checker

A failure during this step may be an indication of an invalid installation of the above products. Error messages can come in different forms including having the Pulse Secure application hang, or having an

error code returned from the software. Pulse secure will also check to see if a newer version of the software is available and prompt you if an update is needed.

If you suspect that the software did not install properly, uninstall the products above from the control panel and try again. Occasionally OS updates will interfere with the functionality of Pulse Secure requiring a reinstall.

Important: Administrative access may be required to reinstall Pulse Secure. If you do not have administrative access to your machine the Pulse Secure setup client may assist with the installation process. Only uninstall the setup client as a last resort to troubleshooting Pulse secure issues. If you continue to have problems you will need to work directly with your company's IT staff to resolve these issues, as installation requires administrative access.

During the software installation process several security prompts will be required to allow the Pulse Secure software to run properly. Be sure to click "ok", "yes", and/or "continue" when presented with these prompts.

Step 3: Host Checker Validation (Up-to-Date Anti-Virus)

Error Message: ***"Your computer's security is unsatisfactory"***

This step includes the validation of the Host Checker on the client computer. The host checker software checks your computer to be sure it meets the necessary security requirements to connect to our network. Host checker messages will be fairly specific in describing what criteria are not satisfactory about your computer. Typically problems include the following.

- Anti-virus vendors will occasionally release versions of their software prior to Pulse Secure being able to include support. Be conscious about version updates to your antivirus software, and hold off installing them until you are certain the version is supported by Pulse Secure. A list of supported AV Software can be found on our Compliant AV Products for Windows OS (ESAP)
- If the host checker is indicating that your virus definitions are out of date, attempt a manual update of virus definitions being sure they are dated within the past 24 hours. Antivirus companies will sometimes release several updates within a short period of time, so you may need to run the update process multiple times.
- In the event your antivirus solution is unsatisfactory, you may find success in switching to a different antivirus package as an immediate solution. Many free antivirus solutions are supported by Pulse Secure. Be careful to not run 2 antivirus products at the same time, this can cause additional issues.

Connection issues can sometimes be related to DNS problems. You can also connect to the VPN with the direct IP address of https://129.164.100.92 (instead of remote.ivv.nasa.gov). If you are prompted to accept a security certificate, please do so. This will bypass DNS settings that may cause problems.

Advanced Troubleshooting Tips for VPN

Each of these steps should be performed independent of each other and your connection tested after each step to determine if the change was successful. The steps should also be performed in the order in which they are listed below. Some of these tips do require admin rights to your device to perform the change.

Troubleshooting Step 1: Check for Pending Microsoft Updates

1. Go to **Start > Settings > Update & Security >** Click **Check for Updates**
   Note: You may have to perform this more than once depending on how many updates are pending.

Troubleshooting Step 2: Check Juniper Network Service on Adapters *(Admin Rights Required)*

1. You will check to determine if this service is unchecked from all adapters.
   Note: physical and virtual-you will need to be connected to the VPN to uncheck from Pulse Secure Adapter
2. Follow Method 2 in this manual (It will require that you have admin rights on your device):
   https://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB43833

Troubleshooting Step 3: Network Reset *(Admin Rights Required)*

1. Go to **Start > Settings > Network & Internet >** Select **Network Reset**
2. **Reboot Required**

For onsite customers, the IT Services Department offers Remote Desktop connectivity. The following guides will assist you in establishing a remote desktop connection after you have connected to the NASA IV&V SSLVPN service.

Getting Started with Remote Desktop Connection for Windows

A list of supported AV Software can be found on our Compliant AV Products for Windows OS (ESAP).

Guides are available from our internal ITS Remote Access Website and will require a VPN connection to access.

In the event that you are unable to connect to the full VPN, an alternative solution that can give you access to ECM and email, is to use the Web only client. The Web only client is available at https://remote.ivv.nasa.gov/web. The web only client does not support remote desktop connections but will allow you to get to https://portal.office.com for logging into O365.

Contact the IT Help Desk for additional support on connecting to the VPN or if you have any questions when connecting to the VPN at ivv-dl-help@mail.nasa.gov or 304-367-8237.